Serveur de temps NTP

Rémy De Poorter 52063

29 avril 2022

Sommaire

Introduction

Pourquoi utiliser l'heure ?

- Les logs
- La connexion d'un utilisateur
- Une commande sur un site internet
- Synchroniser des robots industriels
- Sauvegardes
- Journalisation

Définir l’heure manuellement

sudo timedatectl set-time “2022-04-21 10:23:42”

sudo timedatectl set-timezone Europe/Bruxelles

Problème : ce n’est pas assez précis

Solution : Le protocole NTP

1971 : 23 ordinateurs connectés et envoie du premier courriel

1983 : adoption de TCP/IP et du mot internet

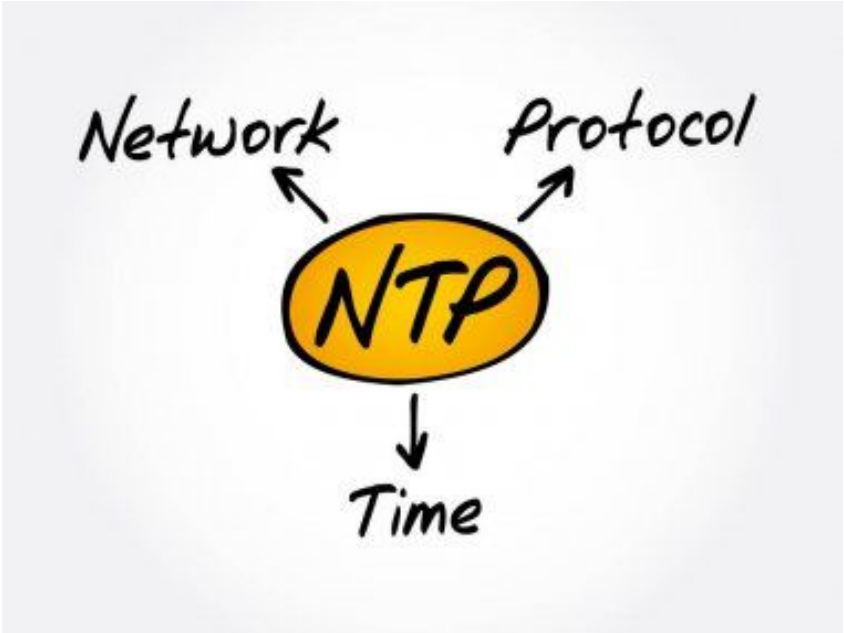
1984 : 1000 ordinateurs connectés

1985 : NTP apparaît

1987 : 10 000 ordinateurs connectés

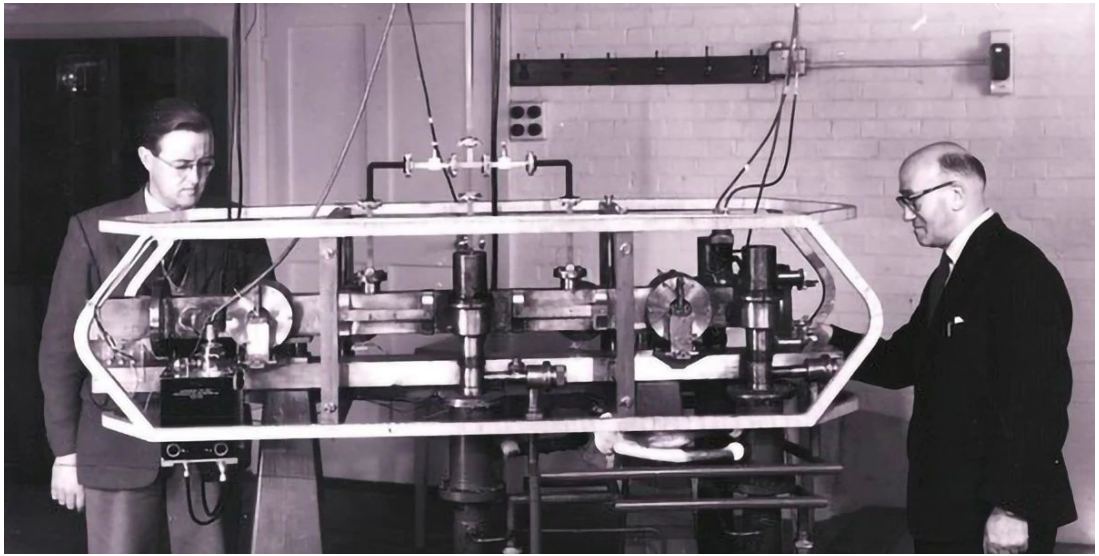
1990 : premier navigateur web

1996 : 36 000 000 ordinateurs connectés.



Horloge atomique

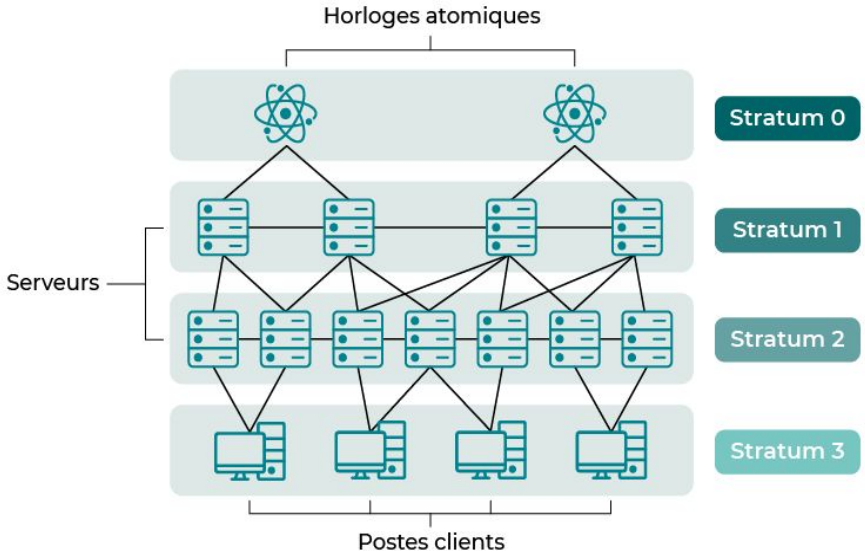
Analyse la fréquence du rayonnement électromagnétique émis par un électron lors du passage d'un niveau d'énergie à un autre.



Cela permet de définir un temps exacte et très stable

Architecture

- Le client se synchronise avec le serveur
- La synchronisation via le réseau ip
- Chaque couche est appelée stratum
- Le plus haut niveau est 0, c’est le plus proche de l'horloge atomique
- Chaque niveau possède un temps fiable, ce qui évite qu’un noeud soit surchargé



Horloge système, logicielle, matérielle RTC

Une horloge système est une horloge logicielle exécutée par le noyau.

Linux utilise une horloge logicielle comme horloge système pour une meilleure résolution que l'horloge matérielle intégrée RTC

Lors du démarrage, l'horloge système lit l'heure et la date à partir de l'heure RTC

L'heure RTC peut se décaler de l'heure réelle jusqu'à 5 minutes par mois à cause des variations de température

D'où le besoin de synchroniser l'horloge système avec des références externes.

Lorsque l'horloge système est synchronisée avec NTP le noyau met automatiquement à jour l'heure RTC

Driftfile

Le fichier de dérive stocke le décalage de fréquence entre l'horloge système exécutée à sa fréquence nominale et la fréquence requise pour rester en synchronisation avec l'heure UTC.

La valeur contenue dans le fichier de dérive est lue pendant le démarrage système et est utilisée pour corriger la source horaire. Cela permet de L'utilisation réduire le temps requis pour atteindre une heure stable et précise.

La valeur est calculée et le fichier de dérive est remplacé une fois par heure par crond.

le driftfile doit donc rester accessible en écriture

Serveur NTP public ou privé

Utilisation interne uniquement ou publique

Un des plus grands clusters public est be.pool.ntp.org

C’est celui la qui est par défaut dans la plupart des distribution Linux.

Belgium — be.pool.ntp.org

To use this specific pool zone, add the following to your ntp.conf file:

```
server 0.be.pool.ntp.org
server 1.be.pool.ntp.org
server 2.be.pool.ntp.org
server 3.be.pool.ntp.org
```

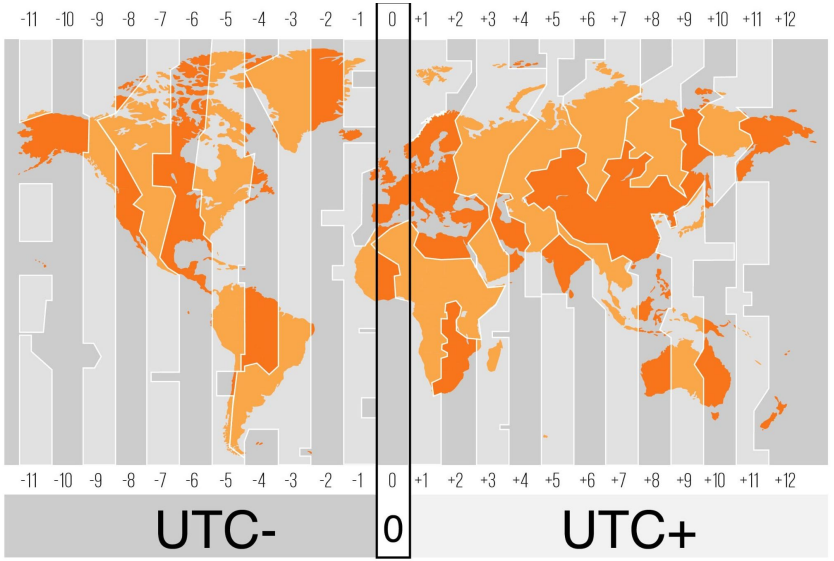
Faut-il obligatoirement configurer son propre serveur ?

Usage de serveur publics est tout à fait possible mais il est intéressant de créer le sien car :

+ meilleures synchronisation entre les serveur de l'entreprise
+ réduction du trafic dû au synchronisation via internet
+ Fiabilité (panne de courant, internet)
+ Indépendance du réseau mondial

NTP ne fait pas tout !

- NTP fournit une heure universelle coordonnée UTC
- C’est l’OS qui gère le changement d’heure et de fuseaux horaires en fonction de la position de la machine cliente
- Les messages ne sont pas cryptés par NTP et circulent librement sur le réseau
- Il est possible de les cryptés mais cela alourdit les paquets à transférer et n’a pas forcément d'intérêt à être sécurisé



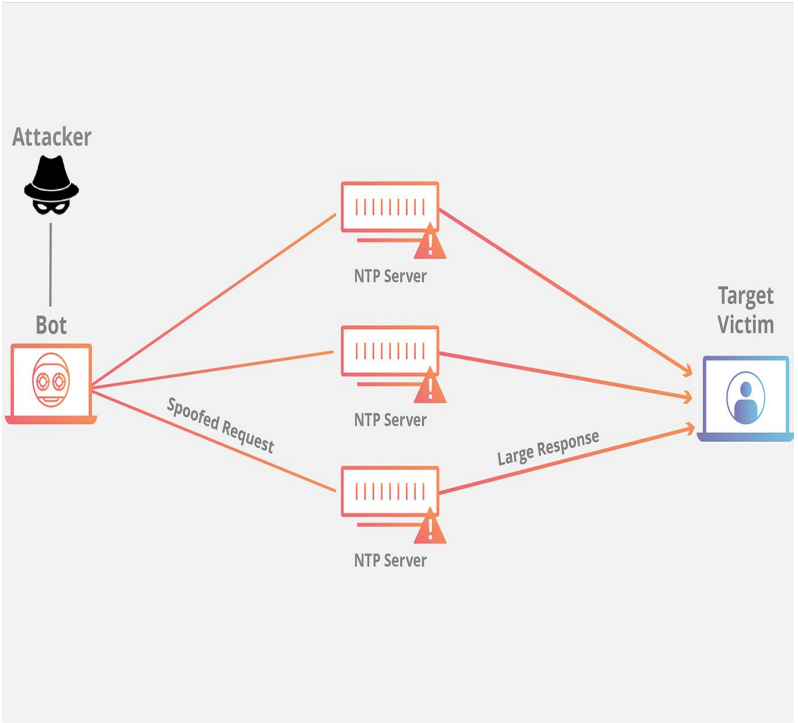
Risque de DDOS - Attaque par amplification NTP

L'attaquant utilise un bot pour envoyer des paquets avec des adresses IP usurpées à un serveur NTP. L'adresse de chaque paquet pointe vers l'adresse ip de la victime

Chaque paquet fait une requête au serveur NTP

Le serveur renvoie sa réponse à l'adresse usurpée avec les données résultantes.

L'adresse IP de la cible reçoit la réponse et l'infrastructure réseau environnante est submergée par un flot de trafic, ce qui entraîne un déni de service.



Comment s’en protéger ?

Rediriger vers un trou noir l’ensemble du traffic destiné a l’adresse IP de la victime.
Ce qui empêche la cible d’avoir accès au site.

Effectuer un filtrage à l’entrée et utiliser un par feu correctement configuré permet d’en être facilement protéger.

Lois de Segal

Un homme avec une montre sait quelle heure il est.
Un homme avec deux montres n'en est jamais sûr.

C’est pourquoi il est conseillé d’avoir au moins 3 serveurs de temps et de les répartir géographiquement. Ainsi l’on aura toujours un temps exacte

Nicolas Hayek
inventeur de la montre swatch

Meilleurs pratiques

- Utiliser des serveur NTP publics pour les hôtes externes
- Configurer son propre serveur ntp interne
- Standardiser le temps UTC
- Restreindre les commandes utilisables sur le serveur stratum.
- Autoriser uniquement les réseaux connus
- Crypté uniquement si c'est nécessaire
- Respecté la loi de Segal
- Si nécessaire ajouter un stratum secondaire pour augmenter la bande passante.
- Faire les mises à jours pour combler les failles et se protéger des attaques réseau

Planificateur de tâche CRON

Exécute une tâche automatiquement à une date et une heure spécifiée
le vendredi 13/01/2022

Ou selon un cycle
tous les ans

Les tâches sont définies dans le fichier /etc/crontab

Elles s'exécutent avec les droits de root sans demander le mot de passe

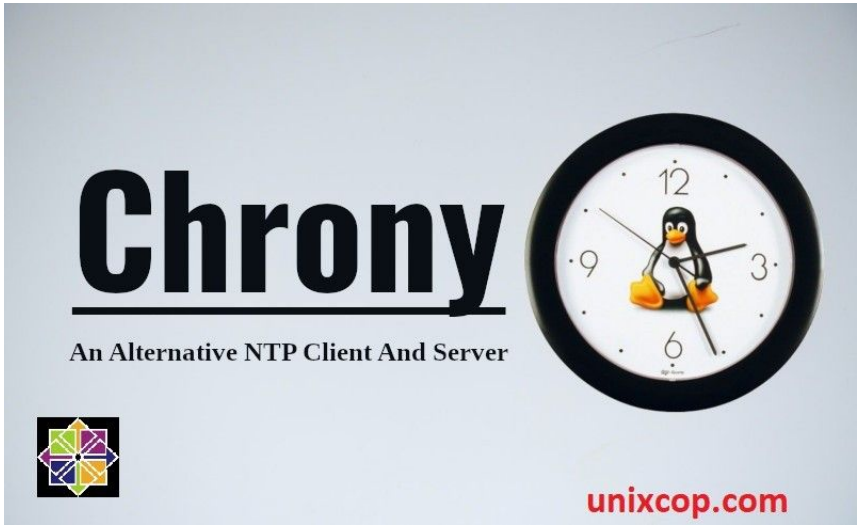
```
# ┌──────────── min (0 - 59)
# │ ┌────────── hour (0 - 23)
# │ │ ┌──────── day of month (1 - 31)
# │ │ │ ┌────── month (1 - 12)
# │ │ │ │ ┌──── day of week (0 - 6) (0 to 6 are Sunday to
# │ │ │ │ │     Saturday, or use names; 7 is also Sunday)
# │ │ │ │ │
# │ │ │ │ │
# * * * * *  command to execute
```

Implémentation d’un serveur NTP local à l’aide de Chrony

Chrony est une implémentation du protocole NTP

Chronyd est un démon exécuter dans l’espace utilisateur

Chronyc est un outil en ligne de commande pour gérer chronyd



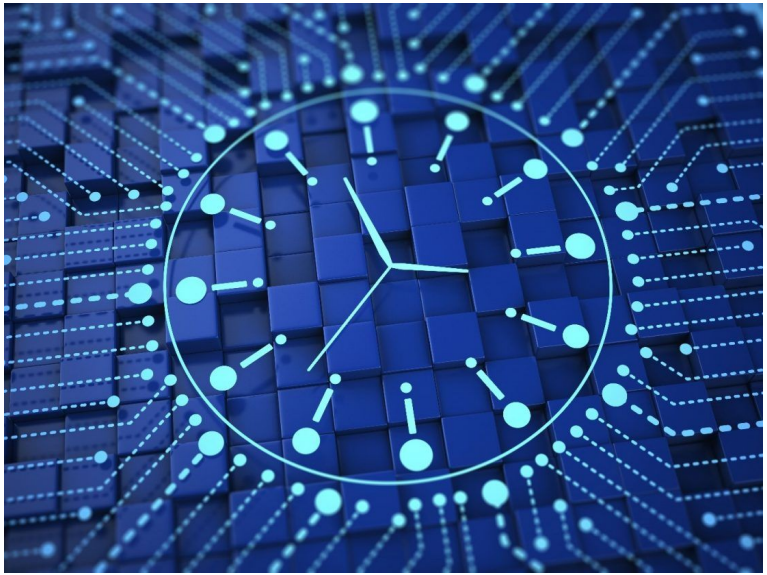
Alternative a NTP le SNTP

- Simple Network Protocole
- Version simplifié de NTP.
- Précision de la seconde.
- Algorithme de traitement plus léger.
- Utilisé pour les systèmes embarqués ou la capacité de calcul est très limitée.
- Communique avec les mêmes serveur que NTP
- Recommandé de l'utiliser que sur des systèmes clients

Conclusion

Protocole ancien et très utilisé à travers le monde qui est un incontournable car :

- Facile à mettre en place
- Très fiable
- A révolutionné les méthodes de paiements, la robotique et la sécurité en ligne en évitant que le client soit réglé à une heure différente de celle du serveur
- Une prochaine version encore + fiable et + précise ?



Question ?